Effective Vulnerability Management

For Government Web Hosting

The web applications, especially of government organizations are prone to malicious attacks intending defamation, service disruption and data corruption. Protection and management of its external facing infrastructure is thus critically important for securing applications and government data.

RATNABOLI GHORAI DINDA
Scientist-F
ratnaboli@nic.in

KASI VISWANATH KETHINENI
Scientist-B
kasiviswanath.k@nic.in

Edited by
MOHAN DAS VISWAM

External facing infrastructures often become the attack surface for malicious users. A web-hosting organization undertakes several steps to keep its infrastructure and services secure, ranging from deploying firewalls to patch management. Security testing process allows revealing the flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. Security requirements include confidentiality, integrity, authentication, availability, authorization and non-repudiation. However, one step that is often overlooked is performing effective Vulnerability Management of its network resources, hosting infrastructure and application services.

The security posture of an organization can be assessed based on vulnerabilities. Even the most secure network is likely to have some unknown vulnerabilities. Vulnerability is a weakness in a program that can lead to an exploit and breach of the network or services by malicious users (attackers). Many cyber-attacks take advantage of basic, often unnoticed security vulnerabilities, such as poor patch management procedures, weak passwords, insecure configurations and non-compliance to sound security policies. This makes an effective Vulnerability Management a critical step in the effort to protect data.

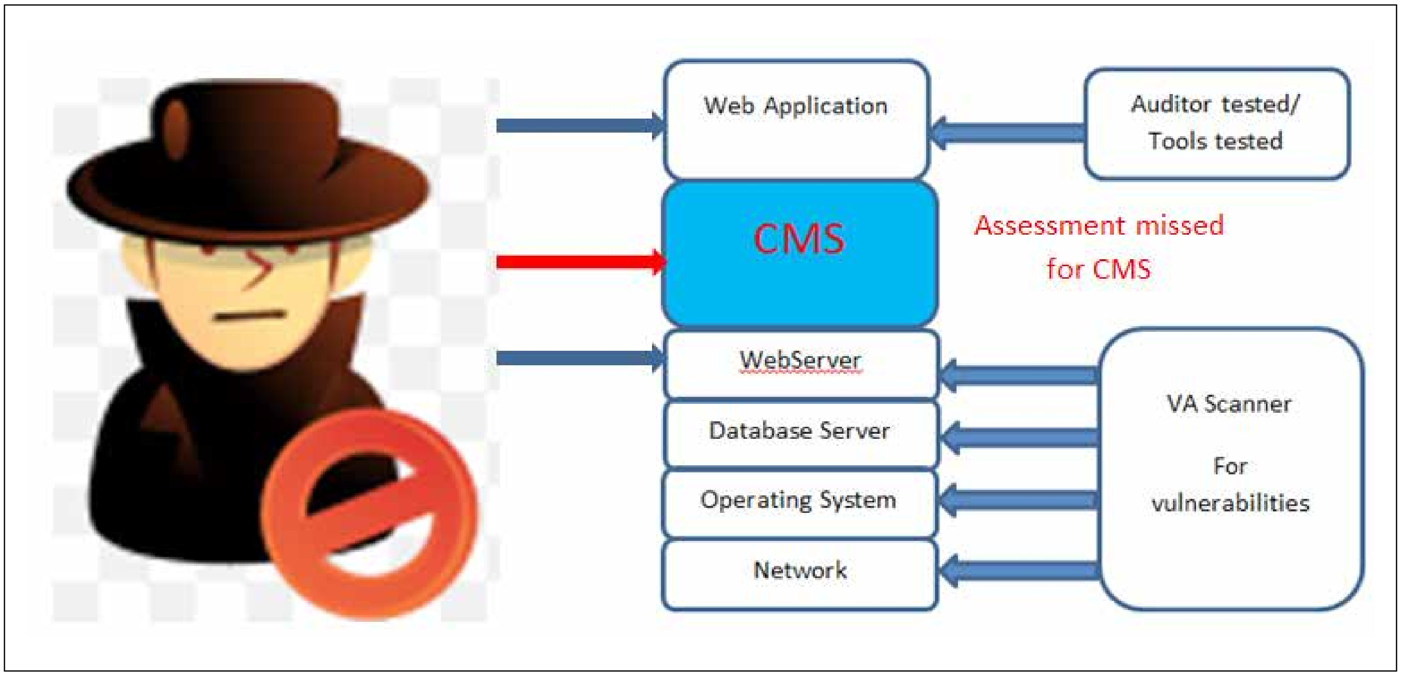
Regular vulnerability assessments are also essential because the security threats continually change and evolve. A public facing application might be secure today, but it could become completely vulnerable tomorrow. This is simply because an attacker would have discovered a previously unknown attack.

VULNERABILITY MANAGEMENT

Vulnerability Management is a security approach to find and mitigate known vulnerabilities by using the security scanners. This process provides in-depth evaluation of the information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk.

Vulnerability assessment is the initial process of identifying and quantifying security vulnerabilities in an environment. Vulnerability Assessments follow these general steps :

- Catalog assets and resources in a system
- Manage assets to maintain vulnerabilities, this requires need to identify the resources attached to the network such as the IP Address database
- Assign quantifiable value and importance to the resources
- Identify the security vulnerabilities or potential threats to each resource using vulnerability scanners



- Validate and prioritize the VA scanner reported vulnerabilities that need to be fixed

VA scanner runs for defined network IPs to find the vulnerabilities. Mitigation or elimination of the vulnerabilities needs to be performed by the administrators. This process of scanning and mitigation should ideally be iterated till patches are fixed completely. In order to perform periodic assessment, this process is usually scheduled to assess the security posture at pre-defined intervals. VA scanners are useful tools for identifying hidden network and host vulnerabilities.

Host based scanners have direct access to the file system on the target host and thus the capability to find low level information on the system like exact version of software installed and services and configuration. These can therefore provide insight into user activities such as using easily guessable passwords or even no password. These can also detect signs that an attacker has already compromised a system, including looking for suspicious file names, unexpected new system files or device files and unexpected privileged programs. Host-based scanners can also perform baseline (or file system) checks.

SECURITY OF CMS APPLICATIONS

In several applications, a layer above the web server, i.e., the Content Management System (CMS) is used in software building for rapid application development. CMS based applications follow the agile methodology to develop applications. These have gained popularity due to their ease of use to create applications. However, malicious adversaries often exploit vulnerabilities within the CMS installed on the web servers of organization. Also, the source code of most popular open source CMSs are publicly available, and can be easily targeted. Once the CMS has been compromised, the web server can be used as infrastructure to facilitate targeted intrusion attempts.

These CMSs may usually be considered low priority in assessment of the security posture of organization. Available VA Scanners usually run for different vulnerabilities of the entire web-stack, as one vulnerable component could compromise the security of the other layers. Vulnerability management scopes assessing of the operating system, webserver, database server, third-party applications or custom site-specific code scanning is not sufficient. The assessment of the CMS is more critical since applications and their usage are completely dependent on the CMS.

Once a CMS has been compromised, adversaries can exploit their access to:

- Obtain access to authenticated and privileged areas of the site.
- Upload malware to the webserver to facilitate remote access, WebShells etc.
- Inject malicious content into legitimate web pages. This could be used to server exploits or malware to visitors or to facilitate infrastructure access remotely.

CASE STUDY

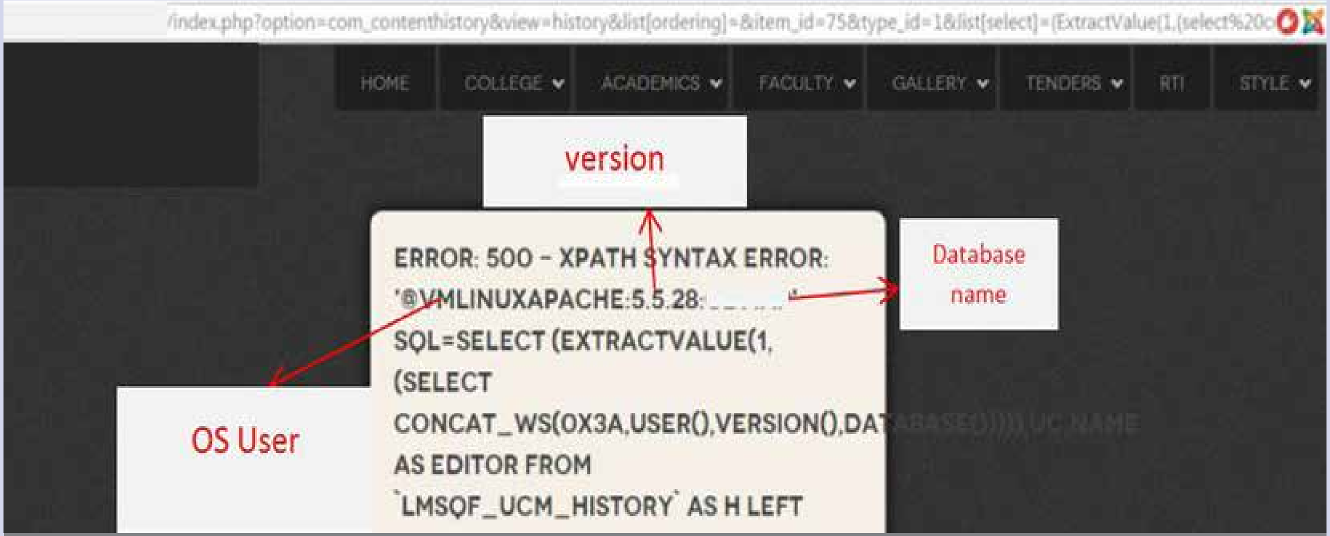
Application vulnerabilities in CMS infrastructure level - JOOMLA

JOOMLA is one of the popular CMS. Different versions of Joomla have different vulnerabilities. Some of these are 0-day vulnerabilities. 0-day attacks are exploits of newly discovered vulnerabilities, caused either before being disclosed to the public or before the necessary patch for the exploit has been applied.

Consider the following example of hardened webserver and OS installed with Joomla CMS. Older versions of the Joomla CMS application have security issues in 'com_contenthistory' module.

The screenshot of the Joomla com_contenthistory shows vulnerability finding using SQL Injection.

```
http://                    /index.php?option=com_contenthistory&view=history&list[ordering]=&ite
m_id=75&type_id=1&list[select]=(ExtractValue(1,(select%20concat_ws(0x3a,user(),version(),database())
)))
```



/index.php?option=com_contenthistory&view=history&list[ordering]=&item_id=75&type_id=1&list[select]=(ExtractValue(1,(select%20c

```
ERROR: 500 - XPATH SYNTAX ERROR:
'@VMLINUXAPACHE:5.5.28: _ _ . . . '
SQL=SELECT (EXTRACTVALUE(1,
(SELECT
CONCAT_WS(0X3A,USER(),VERSION(),DATABASE())))) UC NAME
AS EDITOR FROM
`LMSQF_UCM_HISTORY` AS H LEFT
```

Vulnerable CMS JOOMLA is prone to SQL Injection and leaks the sensitive information like "Operating system user", "Database name" and "Version of Webserver"

This allows compromising all security layers built for these applications.

TESTING OF CMS WITHIN VA SCOPE

In the Vulnerability Management process, the VA Scanner for web applications / network also may not give good results for CMS based applications.

In most cases, the core CMS application may not be tested thoroughly for vulnerabilities. A Common cause of cyber intrusion is running outdated CMS software/untested CMS. These CMSs targeted by attackers lead to zero-day exploits. Vendors may test for security vulnerabilities and release relevant patches, but this mitigation may take time, since patches need to be tested before going to production.

If a VA Scanner is not able to identify the vulnerable issues, then the security team performs manual security testing periodically and manages CMS security vulnerabilities using built vulnerability finding scripts.

CONCLUSION

As part of web hosting security vulnerability Management process, it is necessary to consider the CMS vulnerabilities checked periodically in order to assess the organization's security posture.

It is also suggested to script the deployment of security tools so that all environments have baseline coverage and run regular vulnerability scans against the environments and remediate any vulnerability.

For further information, please contact:
RATNABOLI GHORAI DINDA
Scientist-F & HOD (Application Security)
NIC, CGO Complex, Lodhi Road
New Delhi- 110 003
Email: ratnaboli@nic.in
Phone: 011-24367828